

Statement of Chris Metaxas
CEO – DRN, Inc.
On Behalf of DRN, Inc. and Vigilant Solutions, Inc.
In Opposition to:
HB 5389 – An Act Concerning the Use of An Automated Number Plate Recognition System
Public Safety & Security Committee
Hartford, Connecticut
Tuesday, March 4, 2014

Good afternoon, Senator Hartley, Representative Dargan and members of the Public Safety Committee. My name Chris Metaxas and I am the CEO of DRN, Inc. based in Fort Worth, TX and I am here representing DRN and Vigilant Solutions, our sister company which is located in Livermore, CA.

Vigilant Solutions is one of the largest providers of license plate recognition – or LPR – technology, analytical software, and data to the law enforcement community. DRN is the largest provider of LPR data services to the private sector. The bill before you today, HB 5389 AAC The Use of an Automated Number Plate Recognition System, would have a significant negative impact on the ability of law enforcement in this state to use anonymous LPR data to solve crimes, and it would prevent the private sector in this state from using the data at all to repossess vehicles or investigate insurance fraud and prevent municipalities from aiding in the collection of delinquent taxes.

LPR has been a tremendous tool for law enforcement. It has been used thousands of times to apprehend criminals, thwart abductions and solve crimes.

Just two weeks ago, one of Vigilant's law enforcement customers in Fairfield, Connecticut contacted Vigilant to notify them of an investigative success that week thanks to LPR data we provided. A woman who is 6 months pregnant was leaving a retail store when a man grabbed her purse, jumped into a car and drove off. He dragged the woman who ended up in the hospital. She was able to share a few characters from the license plate with Fairfield Police.

Using Vigilant's system, Fairfield investigators worked the case all night long to try to identify a license plate from the partial information given by the woman. The next afternoon one of the searches identified a plate and historical location information on that plate. Fairfield Police located the vehicle and after a short period of surveillance a man matching the description walked out of a house and into the car along with a woman. He was pulled over and the couple admitted the purse snatching and produced the purse.

This is a typical example of how law enforcement uses historical and privately collected LPR data and Vigilant's analytical software to solve crimes. Within 24 hours, it helped investigators solve a case that would otherwise have been extremely difficult to resolve. We are proud of results like this and even more importantly happy to understand that the pregnant woman is doing fine.

In the private sector, DRN's privately collected LPR data has been used in the repossession of

more than 300,000 vehicles worth more than \$2.2 billion in assets returned, resulting in an impact of 14% on auto lenders' delinquent portfolios. This has lowered risk for lenders, which stabilizes interest rates that consumers pay for their auto loans and enhances the ability of make more affordable loans. In addition, DRN's privately collected LPR data has led to the recovery of more than 37,000 stolen vehicles, which has lowered risk to insurers and had a consumer-friendly impact on insurance premiums.

If you take action to restrict the operation of LPR technology or the retention and use of LPR data as HB 5389 proposes to do, then you are taking away the ability to do these things – both in the public and private sectors.

Proponents of restrictions on the use of LPR cite concerns about massive warrantless tracking by law enforcement. These concerns are a result of wild misinformation, and I am here today to present the real facts so that as you consider this proposed legislation, you have a clear understanding of how the technology works, and how it is used.

LPR is used routinely by law enforcement and the private sector to rescue abducted children, catch murderers, recover missing elderly adults, recover stolen vehicles, repossess cars whose drivers have broken contracts with lending institutions, and investigate insurance fraud.

All of these great things are being done hundreds of times per day – without any abuse of an innocent citizen's privacy.

I am not suggesting that privacy should not be a concern. As a private citizen I don't want the government tracking my movements and using information to intimidate me. However, protections are already in place to prevent misuse of LPR to track innocent citizens.

It is settled law that there is absolutely no expectation of privacy in a license plate. License plates are mandated by law to be mounted and publicly visible. The primary purpose of a license plate is to aid in public identification so that private actors (e.g. witnesses to traffic accidents) and public entities (e.g. the police) can ascertain where a vehicle was and when it was there. LPR technology just automates a process that has been manual. LPR technology takes a picture of a license plate and includes date, time, and location information – just like most other digital photographs that are taken today with a phone and exist in popular sites like Instagram and Facebook.

LPR databases – which people are concerned about – are nothing but a collection of these pictures and date, time, and location the pictures were taken. They do not contain any personally identifiable information.

If I held up a license plate for you right now, there is no way for you to tell me which car it belongs to, yet alone who owns it and where they live. In order to tell me, you would have to get access to the state's registry of motor vehicles. If you accessed that registry to connect personally identifiable information to a license plate photograph, and you did not have an authorized permissible purpose under the law, then you would be breaking the law.

Let me be clear: in order to misuse LPR data you have to break the law to access personal information from a state registry of motor vehicles that ties a license plate to an individual. The federal Drivers Privacy Protection Act already governs access to the DMV data. **The public has not heard this fact nearly enough.**

It is easy to paint a scary picture of what COULD happen if LPR data is abused. And I have seen some egregiously dramatic scenarios that have been publicized to provoke media and public concern. Those scenarios are wildly unrealistic and betray a fundamental misunderstanding of how the data IS used and CAN be used.

Not only that, those scenarios are ALREADY ILLEGAL.

If this committee wants to increase privacy around LPR data, here are some concrete suggestions I would encourage you to consider that would be very effective without taking away the benefits of the technology:

1. Enforce the laws that are already in place for personally identifiable information. This way only those individuals with an expressed permissible purpose can access the data.
2. Make sure LPR data is available to investigators – that means no arbitrary cut-off dates for when the potentially useful and anonymous pictures must be destroyed.
3. Make sure there are strict controls around how LPR data can be accessed by law enforcement and that access is related to a specified case.
4. Make sure there are frequent audits to ensure any unauthorized access or use of the data is identified and punished.
5. Make sure the data is secure from unauthorized access.
6. Make sure LPR data held by law enforcement is classified as protected data that is not subject to random requests from the public.
7. Finally, do not deprive a private entity from taking a photograph of an object in public view. That would be a plain violation of the private entity's First Amendment rights.

These are measures that would clearly protect against mass warrantless surveillance by law enforcement. They would also prevent someone from accessing LPR data to find historical locations of license plate numbers that are already known to them.

Additionally, these measures would preserve law enforcement's ability to use valuable investigative data to do the great work they do – like the work of Fairfield Police two weeks ago.

In closing, DRN and Vigilant Solutions respectfully opposes HB 5389. We look forward to working with you to address the legitimate use of LPR data by other users for collection of taxes, investigation of fraud and the repossession of automobiles.

Thank you for the opportunity to testify today and I look forward to working with the committee as a resource as you consider this proposed legislation.